On Page 3, between lines 8 and 9, please insert the following:

SUMMARY OF THE INVENTION

On Page 33, please delete line 12 and replace with the following:

A1

BRIEF DESCRIPTION OF THE DRAWINGS

FIGS. 1A-1D, 2A, 2B, 3A and 3B are graphs useful in explaining the present invention.

DETAILED DESCRIPTION OF PREFERRED EMBODIMENTS

IN THE CLAIMS

1. (Amended) Method designed to prove to a controller entity,

- the authenticity of an entity and/or
- the integrity of a message M associated with this entity,

A2 Cm't

by means of all or part of the following parameters or derivatives of these parameters:

- m pairs of private values Q_1, Q_2, ... Q_m and public values G_1, G_2, ... G_m (m being greater than or equal to 1),
- a public modulus n constituted by the product of f prime factors p_1, p_2, ... p_f (f being greater than or equal to 2),

the said modulus and the said private and public values being related by relations of the following type

$$G_i . Q_i^v \equiv 1 . \bmod n \text{ or } G_i . \equiv Q_i^v . \bmod n$$

where v denotes a public exponent of the form:

$$v = 2^k$$

where k is a security parameter greater than 1;

the said m public values G_i being squares g_i^2 of m distinct base numbers $g_1, g_2, \ldots g_m$, smaller than the f prime factors $p_1, p_2, \ldots p_m$;

the said $p_1, p_2, \ldots p_m$ prime factors and/or the said m base numbers $g_1, g_2, \ldots g_m$ being produced such that the following conditions are satisfied:

First condition

each of the equations:

$$x^v \equiv g_i^2 \bmod n$$

A2 cm't

can be resolved in x in the ring of integers modulo n;

Second condition

if $G_i \equiv Q_i^v \bmod n$, among the m numbers q_i obtained by taking Q_i squared modulo n, k-1 times, one of them is not equal to $\pm g_i$ (in other words is not trivial),

if $G_i.Q_i^v \equiv 1 \bmod n$, among the m numbers q_i obtained by taking the inverse of Q_i modulo n squared modulo n, k-1 times, one of them is not equal to $\pm g_i$ (in other words is not trivial);

Third condition

at least one of the 2m equations

$$x^2 \equiv g_i \bmod n$$

$$x^2 \equiv -g_i \bmod n$$

can be resolved in x in the ring of integers modulo n;

the said method implements, in the following steps, an entity called a witness having f prime factors pi and/or m numbers of base gi and/or parameters of the Chinese remainders of the prime factors and/or the public modulus *n* and/or the m private values Qi and/or the f.m components $Q_{i,j}$ ($Q_{i,j} \equiv Q_i \bmod p_j$) of the private values Q_i and of the public exponent v;

- the witness computes commitments R in the ring of integers modulo n; each commitment being computed:

. either by performing operations of the type:

$$R \equiv r^v \bmod n$$

where r is a random value such that 0 < r < n,

A2 Cmt

. or

.. by performing operations of the type

$$R_i \equiv r_i^v \bmod p_i$$

where r_i is a random value associated with the prime number P_i such that $0<r_i<P_i$, each r_i belonging to a collection of random values $\{r_1, r_2, \ldots r_f\}$

.. then by applying the Chinese remainders method,

- the witness receives one or more challenges d; each challenge d comprising m integers d_i hereinafter called elementary challenges; the witness, on the basis of each challenge d, computes a response D by performing operations of the type:

$$D \equiv r.Q_1^{d1}.Q_2^{d2} \ldots Q_m^{dm} \bmod n$$

. or

.. by performing operations of the type:

$$D_i \equiv r_i.Q_{i,1}^{d1}.Q_{i,2}^{d2} \ldots Q_{i,m}^{dm} \bmod p_i$$

.. then by applying the Chinese remainders method;

the said method being such that there are as many responses D as there are challenges d as there are commitments R, each group of numbers R, d, D forming a triplet referenced {R,d,D}.

2. (Amended) Method according to claim 1, designed to prove the authenticity of an entity known as a demonstrator to an entity known as the controller, the said demonstrator entity comprising the witness;

the said demonstrator and controller entities executing the following steps:

A2 Cont

. **Step 1: act of commitment R**

- at each call, the witness computes each commitment R by applying the process specified according to claim 1,

- the demonstrator sends the controller all or part of each commitment R,

. **Step 2: act of challenge d**

- the controller, after having received all or part of each commitment R, produces challenges d whose number is equal to the number of commitments R and sends the challenges d to the demonstrator,

. **Step 3: act of response D**

- the witness computes the responses D from the challenges d by applying the process specified according to claim 1,

. **Step 4: act of checking**

- the demonstrator sends each response D to the controller,

case where the demonstrator has transmitted a part of each commitment R if the demonstrator has transmitted a part of each commitment R, the controller, having the m public values G_1, G_2 ..., G_m, computes a reconstructed commitment R', from each challenge d and each response D, this reconstructed commitment R' satisfying a relationship of the type:

$$R' \equiv G_1^{d1}.G_2^{d2}. \ldots G_m^{dm}. D^v \bmod n$$

or a relationship of the type

$$R' \equiv D^v/G_1^{d1}.G_2^{d2}. \ldots G_m^{dm}. \bmod n$$

the controller ascertains that each reconstructed commitment R' reproduces all or part of each commitment R that has been transmitted to it,

A2 cont

case where the demonstrator has transmitted the totality of each commitment R

if the demonstrator has transmitted the totality of each commitment R, the controller, having the m public values G_1, G_2,... G_m, ascertains that each commitment R satisfies a relationship of the type

$$R' \equiv G_1^{d1}.G_2^{d2}. \ldots G_m^{dm}. D^v \bmod n$$

or a relationship *of* the type

$$R' \equiv D^v/G_1^{d1}.G_2^{d2}. \ldots G_m^{dm}. \bmod n.$$

Claims 3 and 4 are not changed.

5. (Amended) Method according to claim 4, designed to prove the authenticity of the message M by checking the signed message through an entity called a controller;

Checking operation

the said controller entity having the signed message executes a checking operation by proceeding as follows:

. **case where the controller has commitments R, challenges d, responses D,**

if the controller has commitments R, challenges d, responses D,

. . the controller ascertains that the commitments R, the challenges d and the responses D satisfy relationships of the type

A2 Cont

$$R \equiv G_1^{d1} . G_2^{d2} . \dots G_m^{dm} . D^v \bmod n$$

or relationships of the type

$$R \equiv D^v / G_1^{d1} . G_2^{d2} . \dots G_m^{dm} . \bmod n$$

. . the controller ascertains that the message M, the challenges d and the commitments R satisfy the hashing function

$$d = h\ (\text{message}, R)$$

. **case where the controller has challenges d and responses D**

if the controller has challenges d and responses D,

. . the controller reconstructs, on the basis of each challenge d and response D, commitments R' satisfying relationships of the type:

$$R' \equiv G_1^{d1} . G_2^{d2} . \dots G_m^{dm} . D^v \bmod n$$

or relationships of the type

$$R' \equiv D^v / G_1^{d1} . G_2^{d2} . \dots G_m^{dm} . \bmod n$$

. . the controller ascertains that the message M and the challenges d satisfy the hashing function

$$d=h(\text{message},R')$$

. **case where the controller has commitments R and responses D**

if the controller has commitments R and responses D,

. . the controller applies the hashing function and reconstructs d'

$$d' = h\ (\text{message},\ R)$$

. . the controller ascertains that the commitments R, the challenges d' and the responses D satisfy relationships of the type:

$$R \equiv G_1^{d1}.G_2^{d2}.\ \ldots\ G_m^{dm}.\ D^v \bmod n$$

or relationships of the type

$$R \equiv D^v/G_1^{d1}.G_2^{d2}.\ \ldots\ G_m^{dm}.\ \bmod n.$$

A2
Cont

6. (Amended) System designed to prove, to a controller server,

- the authenticity of an entity and/or

- the integrity of a message M associated with this entity,

by means of all or part of the following parameters or derivatives of these parameters:

- m pairs of private values Q_1, Q_2, ... Q_m and public values G_1, G_2, ... G_m (m being greater than or equal to 1),

- a public modulus n constituted by the product of f prime factors p_1, p_2, ... p_f (f being greater than or equal to 2),

the said modulus and the said private and public values being related by relations of the following type:

$$G_i . Q_i^v \equiv 1. \bmod n \text{ or } G_i \equiv Q_i^v \bmod n;$$

where v denotes a public exponent of the form:

$$v = 2^k$$

where k is a security parameter greater than 1;

the said m public values G_i being squares g_i^2 of m distinct base numbers $g_1, g_2, \ldots g_m$, smaller than the f prime factors $p_1, p_2, \ldots p_f$;

the said $p_1, p_2, \ldots p_f$ prime factors and/or the said m base numbers $g_1, g_2, \ldots g_m$ being produced such that the following conditions are satisfied:

A2 Cnt

First condition

each of the equations:

$$x^v \equiv g_i^2 \bmod n$$

can be resolved in x in the ring of integers modulo n;

Second condition

if $G_i \equiv Q_i^v \bmod n$, among the m numbers q_i obtained by taking Q_i squared modulo n, k-1 times, one of them is not equal to $\pm g_i$ (in other words is not trivial),

if $G_i . Q_i^v \equiv 1 \bmod n$, among the m numbers q_i obtained by taking the inverse of Q_i modulo n squared modulo n, k-1 times, one of them is not equal to $\pm g_i$ (in other words is not trivial);

Third condition

at least one of the 2m equations

$$x^2 \equiv g_i \bmod n$$

$$x^2 \equiv -g_i \bmod n$$

can be resolved in x in the ring of integers modulo n;

the said system comprises a witness device, contained especially in a nomad object which, for example, takes the form of a microprocessor-based bank card,

the witness device comprises

- a memory zone containing the f prime factors p_i and/or the m numbers of bases gi and/or parameters of the Chinese remainders of the prime factors and/or the public modulus n and/or the m private values Q_i and/or the f.m components $Q_{i,j}$ ($Q_{i,j} \equiv Q_i \bmod p_j$) of the private values Q_i and of the public exponent v;

A2 cont

the said witness device also comprises:

- random value production means, hereinafter called random value production means of the witness device,

- computation means, hereinafter called means for the computation of commitments R of the witness device, to compute commitments R in the ring of integers modulo n; each commitment being computed:

- either by performing operations of the type:

$$R_i \equiv r^v \bmod n$$

where r is a random value produced by the random value production means, and r is such that $0 < r < n$;

- or by performing operations of the type:

$$R_i \equiv r_i^v \bmod p_i$$

where r_i is a random value associated with the prime number p_i such that $0 < r_i < p_i$ each r_i belonging to a collection of random values $\{r_1, r_2, \ldots r_f\}$

produced by random value production means, then by applying the Chinese remainders method;

the said witness device also comprises:

- reception means hereinafter called the means for the reception of the challenges d of the witness device, to receive one or more challenges d; each challenge d comprising m integers d_i hereinafter called elementary challenges;

- computation means, hereinafter called means for the computation of the responses D of the witness device for the computation, on the basis of each challenge d, of a response D,

A2 cm't

. either by performing operations of the type:

$$D \equiv r.Q_1^{d1}.Q_2^{d2}. \ldots Q_m^{dm} \bmod n$$

. or by performing operations of the type:

$$D \equiv r.Q_{i,1}^{d1}.Q_{i,2}^{d2}. \ldots Q_{i,m}^{dm} \bmod p_i$$

and then by applying the Chinese remainders method,

- transmission means to transmit one or more commitments R and one or more responses D;

there are as many responses D as there are challenges d as there are commitments R, each group of numbers R, d, D forming a triplet referenced {R,d,D}.

7. (Amended) System according to claim 6, designed to prove the authenticity of an entity called a demonstrator and an entity called a controller,

the said system being such that it comprises:

- a demonstrator device associated with the demonstrator entity, the said demonstrator device being

interconnected with the witness device by interconnection means and possibly taking the form especially of logic microcircuits in a nomad object, for example the form of a microprocessor in a microprocessor-based bank card,

- a controller device associated with the controller entity, the said controller device especially taking the form of a terminal or remote server, the said controller device comprising connection means for its electrical, electromagnetic, optical or acoustic connection, especially through a data-processing communications network, to the demonstrator device;

A2 Cont

the said system enabling the execution of the following steps:

. **Step 1: act of commitment R**

at each call, the means of computation for the commitments R of the witness device compute each commitment R by applying the process specified according to claim 1,

the witness device has means of transmission, hereinafter called the transmission means of the witness device, to transmit all or part of each commitment R to the demonstrator device through the interconnection means,

the demonstrator device also has transmission means, hereinafter called the transmission means of the demonstrator device, to transmit all or part of each commitment R to the controller device through the connection means;

. **Step 2: act of challenge d**

the controller device comprises challenge production means for the production, after receiving all or part of each commitment R, of the challenges d equal in number to the number of commitments R,

the controller device also has transmission means, hereinafter denoted transmission means of the controller, to transmit challenges d to the demonstrator through connection means,

. **Step 3: act of response D**

the means of reception of the challenges d of the witness device receive each challenge d coming from the demonstrator device through the interconnection means,

A2 Cont

the means of computation of the responses D of the witness device compute the responses D from the challenges d by applying the process specified according to claim 1,

. **Step 4: act of checking**

the transmission means of the demonstrator transmit each response D to the controller,

the controller device also comprises:

- computation means, hereinafter called the computation means of the controller device,

- comparison means, hereinafter called the comparison means of the controller device,

case where the demonstrator has transmitted a part of each commitment R

if the transmission means of the demonstrator have transmitted a part of each commitment R, the computation means of the controller device, having m public values G_1, G_2, ..., G_m, compute a reconstructed commitment R', from each challenge d and each response

10089662 .021803

D, this reconstructed commitment R' satisfying a relationship of the type:

$$R' \equiv G_1^{d1}.G_2^{d2}. \ldots G_m^{dm}. D^v \bmod n$$

or a relationship of the type

$$R' \equiv D^v/G_1^{d1}.G_2^{d2}. \ldots G_m^{dm}. \bmod n$$

the comparison means of the controller device compare each reconstructed commitment R' with all or part of each commitment R received,

case where the controller has transmitted the totality of each commitment R

if the transmission means of the demonstrator have transmitted the totality of each commitment R, the computation means and the comparison means of the controller device, having m public values G_1, G_2, ..., G_m ascertain that each commitment R satisfies a relationship of the type

A2 cont

$$R \equiv G_1^{d1}.G_2^{d2}. \ldots G_m^{dm}. D^v \bmod n$$

or a relationship of the type

$$R \equiv D^v/G_1^{d1}.G_2^{d2}. \ldots G_m^{dm}. \bmod n.$$

8. (Amended) System according to claim 6, designed to give proof to an entity known as a controller, of the integrity of a message M associated with an entity known as a demonstrator,

the said system being such that it comprises

- a demonstrator device associated with the demonstrator entity, the said demonstrator device being interconnected with the witness device by interconnection means and possibly taking the form especially of logic microcircuits in a nomad object,

for example the form of a microprocessor in a microprocessor-based bank card,

- a controller device associated with the controller entity, the said controller device especially taking the form of a terminal or remote server, the said controller device comprising connection means for its electrical, electromagnetic, optical or acoustic connection, especially through a data processing communications network, to the demonstrator device;

the said system enabling the execution of the following steps:

A2 con't

. **Step 1: act of commitment R**

at each call, the means of computation of the commitments R of the witness device compute each commitment R by applying the process specified according to claim 1,

the witness device has transmission means, hereinafter called the transmission means of the witness device, to transmit all or part of each commitment R to the demonstrator device through the interconnection means,

. **Step 2: act of challenge d**

the demonstrator device comprises computation means, hereinafter called the computation means of the demonstrator, applying a hashing function h whose arguments are the message M and all or part of each commitment R to compute at least one token T,

the demonstrator device also has transmission means, hereinafter known as the transmission means of

the demonstrator device, to transmit each token T through the connection means to the controller device,

the controller device also has challenge production means for the production, after having received the token T, of the challenges d in a number equal to the number of commitments R,

the controller device also has transmission means, hereinafter called the transmission means of the controller, to transmit the challenges d to the demonstrator through the connection means;

. **Step 3: act of response D**

A2 cm't

the means of reception of the challenges d of the witness device receive each challenge d coming from the demonstrator device through the interconnection means,

the means of computation of the responses D of the witness device compute the responses D from the challenges d by applying the process specified according to claim 1,

. **Step 4: act of checking**

the transmission means of the demonstrator transmit each response D to the controller,

the controller device also comprises computation means, hereinafter called the computation means of the controller device, having m public values G_1, G_2, ..., G_m, in order to firstly compute a reconstructed commitment R', from each challenge d and each response D, this reconstructed commitment R' satisfying a relationship of the type:

$$R' \equiv G_1^{d1} . G_2^{d2} . \ldots G_m^{dm} . D^v \bmod n$$

or a relationship *of* the type

$$R' \equiv D^v/G_1^{d1}.G_2^{d2}. \ldots G_m^{dm}. \bmod n$$

then, secondly, compute a token T' by applying the hashing function h having as arguments the message M and all or part or each reconstructed commitment R',

the controller device also has comparison means, hereinafter known as the comparison means of the controller device, to compare the token T' with the received token T.

Claim 9 is not changed.

A2 cont

10. (Amended) System according to claim 9, designed to prove the authenticity of the message M by checking the signed message by means of an entity called the controller;

Checking operation

the said system being such that it comprises a controller device associated with the controller entity, the said controller device especially taking the form of a terminal or remote server, the said controller device comprising connection means for its electrical, electromagnetic, optical or acoustic connection, especially through a data-processing communications network, to the signing device;

the said signing device associated with the signing entity comprises transmission means, hereinafter known as the transmission means of the signing device, for the transmission, to the controller device, of the signed message through the connection means, in such a way that the controller device has a signed message comprising:

- the message M,
- the challenges d and/or the commitments R,
- the responses D;

the controller device comprises:

- computation means hereinafter called the computation means of the controller device,
- comparison means, hereinafter called the comparison means of the controller device;

. case where the controller device has commitments R, challenges d, responses D

A2 cont

if the controller has commitments R, challenges d, responses D,

. . the computation and comparison means of the controller device ascertain that the commitments R, the challenges d and the responses D satisfy relationships of the type

$$R \equiv G_1^{d1}.G_2^{d2}. \dots G_m^{dm}. D^v \bmod n$$

or a relationship of the type

$$R \equiv D^v/G_1^{d1}.G_2^{d2}. \dots G_m^{dm}. \bmod n$$

. . the computation and comparison means of the controller device ascertain that the message M, the challenges d and the commitments R satisfy the hashing function:

$$d = h \text{ (message, R)}$$

. case where the controller device has challenges d and responses D

if the controller device has challenges d and responses D,

. . the computation means of the controller device, on the basis of each challenge d and each

response D, compute commitments R' satisfying relationships of the type:

$$R \equiv G_1^{d1}.G_2^{d2}. \dots G_m^{dm}. D^v \bmod n$$

or a relationship of the type

$$R \equiv D^v/G_1^{d1}.G_2^{d2}. \dots G_m^{dm}. \bmod n$$

. . the computation and comparison means of the controller device ascertain that the message M and the challenges d satisfy the hashing function:

$$d = h\ (\text{message}, R')$$

A2 cm't

case where the controller device has commitments R and responses D

if the controller device has commitments R and responses D,

. . the computation means of the controller device apply the hashing function and compute d' such that

$$d' = h\ (\text{message}, R)$$

. . the computation and comparison means of the controller device ascertain that the commitments R, the challenges d' and the responses D satisfy relationships of the type:

$$R \equiv G_1^{d1}.G_2^{d2}. \dots G_m^{dm}. D^v \bmod n$$

or a relationship of the type

$$R \equiv D^v/G_1^{d1}.G_2^{d2}. \dots G_m^{dm}. \bmod n.$$

11. (Amended) Terminal device associated with an entity, taking the form especially of a nomad object, for example the form of a microprocessor in a microprocessor-based bank card, designed to prove to a controller device:

- the authenticity of an entity and/or

- the integrity of a message M associated with this entity;

by means of all or part of the following parameters or derivatives of these parameters:

m pairs of private values Q_1, Q_2, ... Q_m and public values G_1,G_2, ... G_m (m being greater than or equal to 1),

- a public modulus n constituted by the product of f prime factors p_1, p_2, ... p_f (f being greater than or equal to 2),

A2 cont

the said modulus and the said private and public values being related by relations of the following type

$$Gi.Q_i^v \equiv 1 \bmod n \text{ or } Gi \equiv Q_i^v \bmod n;$$

where v denotes a public exponent of the form:

$$v = 2^k$$

where k is a security parameter greater than 1:

the said m public values G_i being squares g_i^2 of m distinct base numbers g_1, g_2, … g_m, smaller than the f prime factors p_1, p_2, … p_f;

the said p_1, p_2, … p_f prime factors and/or the said m base numbers g_1, g_2, … g_m being produced such that the following conditions are satisfied:

First condition

each of the equations:

$$x^v \equiv g_i^2 \bmod n$$

can be resolved in x in the ring of integers modulo n

Second condition

if $Gi \equiv Q_i^v \bmod n$, among the m numbers q_i obtained by taking Q_i squared modulo n, k-1 times, one of them is not equal to $\pm g_i$ (in other words is not trivial),

if $G_i.Q_i^v \equiv 1 \bmod n$, among the m numbers q_i obtained by taking the inverse of Q_i modulo n squared modulo n, k-1 times, one of them is not equal to $\pm g_i$ (in other words is not trivial);

Third condition

at least one of the 2m equations

$$x^2 \equiv g_i \bmod n$$

$$x^2 \equiv -g_i \bmod n$$

can be resolved in x in the ring of integers modulo n;

A2 cont

the said terminal device comprises a witness device comprising

- a memory zone containing the f prime factors p_i and/or the m numbers of bases g_i and/or parameters of the Chinese remainders of the prime factors and/or the public modulus n and/or the m private values Q_i and/or the f.m components $Q_{i,j}$ ($Q_{i,j} \equiv Q_i \bmod p_j$) of the private values Q_i and of the public exponent v;

the said witness device also comprises:

- random value production means, hereinafter called random value production means of the witness device,

- computation means, hereinafter called means for the computation of commitments R of the witness device,

to compute commitments R in the ring of integers modulo n; each commitment being computed:

- either by performing operations of the type:

$$R \equiv r^v \bmod n$$

where r is a random value produced by the random value production means, and r is such that $0 < r < n$.

- or by performing operations of the type:

$$R_i \equiv r_i^v \bmod p_i$$

where r_i is a random value associated with the prime number p_i such that $0 < r_i < p_i$ each r_i belonging to a collection of random values $\{r_1, r_2, \ldots r_f\}$ produced by random value production means, then by applying the Chinese remainders method;

A2 Con't

the said witness device also comprises:

- reception means hereinafter called the means for the reception of the challenges d of the witness device, to receive one or more challenges d; each challenge d comprising m integers d_i hereinafter called elementary challenges;

- computation means, hereinafter called means for the computation of the responses D of the witness device for the computation, on the basis of each challenge d, of a response D,

. either by performing operations of the type:

$$D \equiv r.Q_1^{d1}.Q_2^{d2}. \ldots Q_m^{dm} \bmod n$$

. or by performing operations of the type:

$$D \equiv r.Q_{i,1}^{d1}.Q_{i,2}^{d2}. \ldots Q_{i,m}^{dm} \bmod p_i$$

and then by applying the Chinese remainders method.

- transmission means to transmit one or more commitments R and one or more responses D;

there are as many responses D as there are challenges d as there are commitments R, each group of numbers R, d, D forming a triplet referenced {R, d, D}.

Claims 12-14 are not changed.

15. (Amended) Controller device especially taking the form of a terminal or remote server associated with a controller entity, designed to prove:

- the authenticity or an entity and/or

A2 Cont

- the integrity of a message M associated with this entity.

by means of all or part of the following parameters or derivatives of these parameters:

- m pairs of public values $G_1, G_2, \ldots G_m$ (m being greater than or equal to 1),

- a public modulus n constituted by the product of f prime factors $p_1, p_2, \ldots p_f$ (f being greater than or equal to 2), unknown to the controller device and the associated controller entity,

the said modulus and the said private and public values being related by relations of the following type

$$G_i . Q_i^v \equiv 1. \bmod n \text{ or } G_i \equiv Q_i^v \bmod n;$$

where v denotes a public exponent of the form:

$$v = 2^k$$

where k is a security parameter greater than 1;

where Q_i is a private value, unknown to the controller device, associated with the public value G_i;

the said m public values G_i being squares g_i^2 of m distinct base numbers $g_1, g_2, \ldots g_m$, smaller than the f prime factors $p_1, p_2, \ldots p_f$;

the said $p_1, p_2, \ldots p_f$ prime factors and/or the said m base numbers $g_1, g_2, \ldots g_m$ being produced such that the following conditions are satisfied:

First condition

each of the equations:

$$x^v \equiv g_i^2 \bmod n$$

can be resolved in x in the ring of integers modulo n

A2 cm. X

Second condition

if $G_i \equiv Q_i^v \bmod n$, among the m numbers q_i obtained by taking Q_i squared modulo n, k-1 times, one of them is not equal to $\pm g_i$ (in other words is not trivial),

if $G_i.Q_i^v \equiv 1 \bmod n$, among the m numbers q_i obtained by taking the inverse of Q_i modulo n squared modulo n, k-1 times, one of them is not equal to $\pm g_i$ (in other words is not trivial);

Third condition

at least one of the 2m equations

$$x^2 \equiv g_i \bmod n$$

$$x^2 \equiv -g_i \bmod n$$

can be resolved in x in the ring of integers modulo n.

16. (Amended) Controller device according to claim 15, designed to prove the authenticity of an entity called a demonstrator to an entity called a controller;

the said controller device comprising connection means for its electrical, electromagnetic, optical or acoustic connection, especially through a data-processing communications network, to a demonstrator device associated with the demonstrator entity;

the said controller device being used to execute the following steps:

. **Steps 1 and 2; act of commitment R, act of challenge d**

A2 cont

the said controller device also has means for the reception of all or part of the commitments R coming from the demonstrator device through the connection means,

the controller device has challenge production means for the production, after receiving all or part of each commitment R, of the challenges d in a number equal to the number of commitments R, each challenge d comprising m integers di hereinafter called elementary challenges,

the controller device also has transmission means, hereinafter called transmission means of the controller, to transmit the challenges d to the demonstrator through the connection means;

. **Steps 3 and 4: act of response, act of checking**

the said controller device also comprises:

- means for the reception of the responses D coming from the demonstrator device, through the connection means,

- computation means, hereinafter called the computation means of the controller device,

- comparison means, hereinafter called the comparison means of the controller device,

case where the demonstrator has transmitted a part of each commitment R

if the reception means of the demonstrator have received a part of each commitment R, the computation means or the controller device, having m public values G_1, G_2, ..., G_m compute a reconstructed commitment R', from each challenge d and each response D, this reconstructed commitment R' satisfying a relationship of the type:

Ab cn.t

$$R' \equiv G_1^{d1}.G_2^{d2}. \ldots G_m^{dm}. D^v \bmod n$$

or a relationship of the type

$$R' \equiv D^v/G_1^{d1}.G_2^{d2}. \ldots G_m^{dm}. \bmod n$$

the comparison means of the controller device compare each reconstructed commitment R' with all or part of each commitment R received,

case where the demonstrator has transmitted the totality of each commitment R

if the reception means of the controller device have received the totality of each commitment R, the computation means and the comparison means of the controller device, having m public values G_1, G_2, ..., G_m ascertain that each commitment R satisfies a relationship of the type:

$$R \equiv G_1^{d1}.G_2^{d2}. \ldots G_m^{dm}. D^v \bmod n$$

or a relationship *of* the type

$$R \equiv D^v / G_1^{d1} . G_2^{d2} . \dots G_m^{dm} . \bmod n.$$

Claim 17 is not changed.

18. (Amended) Controller device according to claim 15, designed to prove the authenticity of the message M by checking a signed message by means of an entity called a signed message;

the signed message sent by a signing device associated with a signing entity having a hashing function h (message, R), comprising:

A2 cnt

- the message M,
- the challenges d and/or the commitments R,
- the response D;

Checking operation

the said controller device comprising connection means for its electrical, electromagnetic, optical or acoustic connection, especially through a data-processing communications network, to a signing device associated with the signing entity, the said controller device having received the signed message from the signing device, through the connection means,

the controller device comprises:

- computation means, hereinafter called the computation means of the controller device,
- comparison means, hereinafter called the comparison means of the controller device;

. **case where the controller device has commitments R, challenges d, responses D**

if the controller has commitments R, challenges d, responses D,

. . the computation and comparison means of the controller device ascertain that the commitments R, the challenges d and the responses D satisfy relationships of the type

$$R \equiv G_1^{d1} . G_2^{d2} . \dots G_m^{dm} . D^v \bmod n$$

or a relationship of the type

$$R \equiv D^v / G_1^{d1} . G_2^{d2} . \dots G_m^{dm} . \bmod n$$

A2 cncld.

. . the computation and comparison means of the controller device ascertain that the message M and the challenges d satisfy the hashing function

$$d = h \text{ (message, R)}$$

A2

. case where the controller device has commitments R and responses D

if the controller device has commitments R and responses D,

. . the computation means of the controller device apply the hashing function and compute d' such that

$$d' = h \text{ (message, R')}$$

. . the computation and comparison means of the controller device ascertain that the commitments R, the challenges d' and the responses D satisfy relationships of the type:

$$R \equiv G_1^{d1} . G_2^{d2} . \dots G_m^{dm} . D^v \bmod n$$

or a relationship of the type

$$R \equiv D^v / G_1^{d1} . G_2^{d2} . \dots G_m^{dm} . \bmod n.$$